SYNOPSYS®

# Coverity Support for OWASP Top 10 (2017)

## C/C++

| Coverity Version 2021.03 - C/C++ | | | |
|---|---|---|---|
| **Category** | **CWE** | **Description** | **Coverity Checker** |
| A1: Injection | 77 | Improper Neutralization of Special Elements used in a Command ('Command Injection') | CERT STR02-C, HEADER_INJECTION, OS_CMD_INJECTION |
| | 78 | Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection') | OS_CMD_INJECTION |
| | 88 | Improper Neutralization of Argument Delimiters in a Command ('Argument Injection') | HEADER_INJECTION, OS_CMD_INJECTION |
| | 89 | Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') | SQLI |
| | 91 | XML Injection (aka Blind XPath Injection) | XPATH_INJECTION |
| | 943 | Improper Neutralization of Special Elements in Data Query Logic | SQLI, XPATH_INJECTION |
| | 1027 | Injection | URL_MANIPULATION |
| A2: Broken Authentication | 287 | Improper Authentication | HARDCODED_CREDENTIALS, SENSITIVE_DATA_LEAK, UNENCRYPTED_SENSITIVE_DATA, WEAK_GUARD |
| | 256 | Unprotected Storage of Credentials | SENSITIVE_DATA_LEAK, UNENCRYPTED_SENSITIVE_DATA |
| | 522 | Insufficiently Protected Credentials | SENSITIVE_DATA_LEAK, UNENCRYPTED_SENSITIVE_DATA |
| | 523 | Unprotected Transport of Credentials | SENSITIVE_DATA_LEAK, UNENCRYPTED_SENSITIVE_DATA |
| | 1028 | Broken Authentication | WEAK_PASSWORD_HASH |
| A3: Sensitve Data Exposure<br>(cont. on next page) | 311 | Missing Encryption of Sensitive Data | CERT MSC18-C, HARDCODED_CREDENTIALS, SENSITIVE_DATA_LEAK, UNENCRYPTED_SENSITIVE_DATA |
| | 312 | Cleartext Storage of Sensitive Information | HARDCODED_CREDENTIALS, SENSITIVE_DATA_LEAK, UNENCRYPTED_SENSITIVE_DATA |
| | 319 | Cleartext Transmission of Sensitive Information | CERT MSC18-C, SENSITIVE_DATA_LEAK, UNENCRYPTED_SENSITIVE_DATA |
| | 320 | Key Management Errors | HARDCODED_CREDENTIALS |
| | 326 | Inadequate Encryption Strength | RISKY_CRYPTO |

| | | | |
|---|---|---|---|
| A3: Sensitve Data Exposure (cont.) | 327 | Use of a Broken or Risky Cryptographic Algorithm | RISKY_CRYPTO, WEAK_PASSWORD_HASH |
| | 328 | Reversible One-Way Hash | RISKY_CRYPTO |
| | 359 | Exposure of Private Personal Information to an Unauthorized Actor | SENSITIVE_DATA_LEAK, UNENCRYPTED_SENSITIVE_DATA |
| A5: Broken Access Control | 22 | Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') | PATH_MANIPULATION |
| | 284 | Improper Access Control | AUTOSAR C++14 A20-8-2, AUTOSAR C++14 A20-8-3, AUTOSAR C++14 A20-8-4, AUTOSAR C++14 A20-8-7, CERT POS37-C, HARDCODED_CREDENTIALS, RISKY_CRYPTO, SENSITIVE_DATA_LEAK, SQLI, UNENCRYPTED_SENSITIVE_DATA, WEAK_GUARD |
| | 285 | Improper Authorization | SQLI |
| | 639 | Authorization Bypass Through User-Controlled Key | SQLI |
| | 1031 | Broken Access Control | URL_MANIPULATION |
| A6: Security Misconfiguration | 16 | Configuration | SENSITIVE_DATA_LEAK, UNENCRYPTED_SENSITIVE_DATA |
| | 209 | Generation of Error Message Containing Sensitive Information | AUTOSAR C++14 A15-3-3, MISRA C++-2008 Rule 15-3-2, SENSITIVE_DATA_LEAK, UNCAUGHT_EXCEPT |

## C#

| Coverity Version 2021.03 - C# | | | |
|---|---|---|---|
| **Category** | **CWE** | **Description** | **Coverity Checker** |
| A1: Injection | 77 | Improper Neutralization of Special Elements used in a Command ('Command Injection') | HEADER_INJECTION, OS_CMD_INJECTION |
| | 78 | Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection') | OS_CMD_INJECTION |
| | 88 | Improper Neutralization of Argument Delimiters in a Command ('Argument Injection') | HEADER_INJECTION, OS_CMD_INJECTION |
| | 89 | Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') | SQLI, SQL_NOT_CONSTANT |
| | 90 | Improper Neutralization of Special Elements used in an LDAP Query ('LDAP Injection') | LDAP_INJECTION, LDAP_NOT_CONSTANT |
| | 91 | XML Injection (aka Blind XPath Injection) | XML_INJECTION, XPATH_INJECTION |
| | 943 | Improper Neutralization of Special Elements in Data Query Logic | LDAP_INJECTION, LDAP_NOT_CONSTANT, SQLI, SQL_NOT_CONSTANT, XPATH_INJECTION |
| | 1027 | Injection | NOSQL_QUERY_INJECTION, REGEX_INJECTION, SCRIPT_CODE_INJECTION, UNKNOWN_LANGUAGE_INJECTION |

| | | | |
|---|---|---|---|
| A2: Broken Authentication | 287 | Improper Authentication | CONFIG.CONNECTION_STRING_PASSWORD, CONFIG.HARDCODED_CREDENTIALS_AUDIT, CORS_MISCONFIGURATION, CORS_MISCONFIGURATION_AUDIT, HARDCODED_CREDENTIALS, INSECURE_COMMUNICATION, MISSING_AUTHZ, SENSITIVE_DATA_LEAK, UNENCRYPTED_SENSITIVE_DATA |
| | 256 | Unprotected Storage of Credentials | SENSITIVE_DATA_LEAK, UNENCRYPTED_SENSITIVE_DATA |
| | 522 | Insufficiently Protected Credentials | CONFIG.CONNECTION_STRING_PASSWORD, CONFIG.HARDCODED_CREDENTIALS_AUDIT, INSECURE_COMMUNICATION, SENSITIVE_DATA_LEAK, UNENCRYPTED_SENSITIVE_DATA |
| | 523 | Unprotected Transport of Credentials | INSECURE_COMMUNICATION, SENSITIVE_DATA_LEAK, UNENCRYPTED_SENSITIVE_DATA |
| | 1028 | Broken Authentication | CONFIG.ASP_VIEWSTATE_MAC, INSECURE_COOKIE, WEAK_PASSWORD_HASH |
| A3: Sensitive Data Exposure | 311 | Missing Encryption of Sensitive Data | HARDCODED_CREDENTIALS, INSECURE_COMMUNICATION, INSECURE_COOKIE, SENSITIVE_DATA_LEAK, UNENCRYPTED_SENSITIVE_DATA |
| | 312 | Cleartext Storage of Sensitive Information | HARDCODED_CREDENTIALS, SENSITIVE_DATA_LEAK, UNENCRYPTED_SENSITIVE_DATA |
| | 319 | Cleartext Transmission of Sensitive Information | INSECURE_COMMUNICATION, SENSITIVE_DATA_LEAK, UNENCRYPTED_SENSITIVE_DATA |
| | 320 | Key Management Errors | HARDCODED_CREDENTIALS |
| | 326 | Inadequate Encryption Strength | RISKY_CRYPTO |
| | 327 | Use of a Broken or Risky Cryptographic Algorithm | RISKY_CRYPTO, WEAK_PASSWORD_HASH |
| | 328 | Reversible One-Way Hash | RISKY_CRYPTO |
| | 359 | Exposure of Private Personal Information to an Unauthorized Actor | CORS_MISCONFIGURATION, CORS_MISCONFIGURATION_AUDIT, INSECURE_COMMUNICATION, SENSITIVE_DATA_LEAK, UNENCRYPTED_SENSITIVE_DATA |
| | 1029 | Sensitive Data Exposure | ASPNET_MVC_VERSION_HEADER, CONFIG.ASPNET_VERSION_HEADER, CONFIG.COOKIES_MISSING_HTTPONLY, CONFIG.DYNAMIC_DATA_HTML_COMMENT, CONFIG.ENABLED_DEBUG_MODE, CONFIG.ENABLED_TRACE_MODE |

| | | | |
|---|---|---|---|
| A4: XML External Entity | 611 | Improper Restriction of XML External Entity Reference | XML_EXTERNAL_ENTITY |
| | 776 | Improper Restriction of Recursive Entity References in DTDs ('XML Entity Expansion') | XML_EXTERNAL_ENTITY |
| A5: Broken Access Control | 22 | Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') | PATH_MANIPULATION |
| | 284 | Improper Access Control | CONFIG.CONNECTION_STRING_PASSWORD, CONFIG.DEAD_AUTHORIZATION_RULE, CONFIG.HARDCODED_CREDENTIALS_AUDIT, CORS_MISCONFIGURATION, CORS_MISCONFIGURATION_AUDIT, HARDCODED_CREDENTIALS, INSECURE_COMMUNICATION, INSECURE_COOKIE, MISSING_AUTHZ, RISKY_CRYPTO, SENSITIVE_DATA_LEAK, SQLI, SQL_NOT_CONSTANT, UNENCRYPTED_SENSITIVE_DATA |
| | 285 | Improper Authorization | CONFIG.DEAD_AUTHORIZATION_RULE, CORS_MISCONFIGURATION, CORS_MISCONFIGURATION_AUDIT, INSECURE_COOKIE, MISSING_AUTHZ, SQLI, SQL_NOT_CONSTANT |
| | 639 | Authorization Bypass Through User-Controlled Key | SQLI, SQL_NOT_CONSTANT |
| A6: Security Misonfiguration | 16 | Configuration | CONFIG.ASPNET_VERSION_HEADER, CONFIG.ASP_VIEWSTATE_MAC, CONFIG.CONNECTION_STRING_PASSWORD, CONFIG.COOKIES_MISSING_HTTPONLY, CONFIG.DEAD_AUTHORIZATION_RULE, CONFIG.ENABLED_DEBUG_MODE, CONFIG.ENABLED_TRACE_MODE, CONFIG.MISSING_CUSTOM_ERROR_PAGE, INSECURE_COMMUNICATION, SENSITIVE_DATA_LEAK, UNENCRYPTED_SENSITIVE_DATA |
| | 209 | Generation of Error Message Containing Sensitive Information | SENSITIVE_DATA_LEAK |
| A7: Cross Site Scripting (XSS) | 79 | Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') | XSS |
| A8: Insecure Deserialization | 502 | Deserialization of Untrusted Data | UNSAFE_DESERIALIZATION |
| A10: Insufficient Logging & Monitoring | 223 | Omission of Security-relevant Information | UNLOGGED_SECURITY_EXCEPTION |
| | 778 | Insufficient Logging | UNLOGGED_SECURITY_EXCEPTION |

# CUDA

| Coverity Version 2021.03 - CUDA | | | |
|---|---|---|---|
| **Category** | **CWE** | **Description** | **Coverity Checker** |
| A1: Injection (cont. on next page) | 77 | Improper Neutralization of Special Elements used in a Command ('Command Injection') | CERT STR02-C, HEADER_INJECTION, OS_CMD_INJECTION |
| | 78 | Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection') | OS_CMD_INJECTION |
| | 88 | Improper Neutralization of Argument Delimiters in a Command ('Argument Injection') | HEADER_INJECTION, OS_CMD_INJECTION |
| A1: Injection (cont.) | 89 | Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') | SQLI |
| | 91 | XML Injection (aka Blind XPath Injection) | XPATH_INJECTION |
| | 943 | Improper Neutralization of Special Elements in Data Query Logic | SQLI, XPATH_INJECTION |
| | 1027 | Injection | URL_MANIPULATION |
| A2: Broken Authentication | 287 | Improper Authentication | HARDCODED_CREDENTIALS, SENSITIVE_DATA_LEAK, UNENCRYPTED_SENSITIVE_DATA, WEAK_GUARD |
| | 256 | Unprotected Storage of Credentials | SENSITIVE_DATA_LEAK, UNENCRYPTED_SENSITIVE_DATA |
| | 522 | Insufficiently Protected Credentials | SENSITIVE_DATA_LEAK, UNENCRYPTED_SENSITIVE_DATA |
| | 523 | Unprotected Transport of Credentials | SENSITIVE_DATA_LEAK, UNENCRYPTED_SENSITIVE_DATA |
| | 1028 | Broken Authentication | WEAK_PASSWORD_HASH |
| A3: Sensitive Data Exposure | 311 | Missing Encryption of Sensitive Data | CERT MSC18-C, HARDCODED_CREDENTIALS, SENSITIVE_DATA_LEAK, UNENCRYPTED_SENSITIVE_DATA |
| | 312 | Cleartext Storage of Sensitive Information | HARDCODED_CREDENTIALS, SENSITIVE_DATA_LEAK, UNENCRYPTED_SENSITIVE_DATA |
| | 319 | Cleartext Transmission of Sensitive Information | CERT MSC18-C, SENSITIVE_DATA_LEAK, UNENCRYPTED_SENSITIVE_DATA |
| | 320 | Key Management Errors | HARDCODED_CREDENTIALS |
| | 326 | Inadequate Encryption Strength | RISKY_CRYPTO |
| | 327 | Use of a Broken or Risky Cryptographic Algorithm | RISKY_CRYPTO, WEAK_PASSWORD_HASH |
| | 328 | Reversible One-Way Hash | RISKY_CRYPTO |
| | 359 | Exposure of Private Personal Information to an Unauthorized Actor | SENSITIVE_DATA_LEAK, UNENCRYPTED_SENSITIVE_DATA |

| | | | |
|---|---|---|---|
| A5: Broken Access Control | 22 | Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') | PATH_MANIPULATION |
| | 284 | Improper Access Control | AUTOSAR C++14 A20-8-2, AUTOSAR C++14 A20-8-3, AUTOSAR C++14 A20-8-4, AUTOSAR C++14 A20-8-7, CERT POS37-C, HARDCODED_CREDENTIALS, RISKY_CRYPTO, SENSITIVE_DATA_LEAK, SQLI, UNENCRYPTED_SENSITIVE_DATA, WEAK_GUARD |
| | 285 | Improper Authorization | SQLI |
| | 639 | Authorization Bypass Through User-Controlled Key | SQLI |
| | 1031 | Broken Access Control | URL_MANIPULATION |
| A6: Security Misconfiguration | 16 | Configuration | SENSITIVE_DATA_LEAK, UNENCRYPTED_SENSITIVE_DATA |
| | 209 | Generation of Error Message Containing Sensitive Information | AUTOSAR C++14 A15-3-3, MISRA C++-2008 Rule 15-3-2, SENSITIVE_DATA_LEAK, UNCAUGHT_EXCEPT |

## Go

| Coverity Version 2021.03 - Go | | | |
|---|---|---|---|
| **Category** | **CWE** | **Description** | **Coverity Checker** |
| A1: Injection | 77 | Improper Neutralization of Special Elements used in a Command ('Command Injection') | HEADER_INJECTION, OS_CMD_INJECTION, TAINTED_ENVIRONMENT_WITH_EXECUTION |
| | 78 | Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection') | OS_CMD_INJECTION, TAINTED_ENVIRONMENT_WITH_EXECUTION |
| | 88 | Improper Neutralization of Argument Delimiters in a Command ('Argument Injection') | HEADER_INJECTION, OS_CMD_INJECTION |
| | 89 | Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') | SQLI |
| | 91 | XML Injection (aka Blind XPath Injection) | XPATH_INJECTION |
| | 943 | Improper Neutralization of Special Elements in Data Query Logic | SQLI, XPATH_INJECTION |
| | 1027 | Injection | NOSQL_QUERY_INJECTION, URL_MANIPULATION |
| A2: Broken Authentication | 287 | Improper Authentication | HARDCODED_CREDENTIALS, SENSITIVE_DATA_LEAK, UNSAFE_BASIC_AUTH |
| | 256 | Unprotected Storage of Credentials | SENSITIVE_DATA_LEAK |
| | 522 | Insufficiently Protected Credentials | SENSITIVE_DATA_LEAK, UNSAFE_BASIC_AUTH |
| | 523 | Unprotected Transport of Credentials | SENSITIVE_DATA_LEAK |

| | | | |
|---|---|---|---|
| A3: Sensitive Data Exposure | 295 | Improper Certificate Validation | BAD_CERT_VERIFICATION |
| | 311 | Missing Encryption of Sensitive Data | HARDCODED_CREDENTIALS, SENSITIVE_DATA_LEAK, UNSAFE_BASIC_AUTH |
| | 312 | Cleartext Storage of Sensitive Information | HARDCODED_CREDENTIALS, SENSITIVE_DATA_LEAK |
| | 319 | Cleartext Transmission of Sensitive Information | SENSITIVE_DATA_LEAK, UNSAFE_BASIC_AUTH |
| | 320 | Key Management Errors | HARDCODED_CREDENTIALS |
| | 326 | Inadequate Encryption Strength | RISKY_CRYPTO |
| | 327 | Use of a Broken or Risky Cryptographic Algorithm | RISKY_CRYPTO |
| | 328 | Reversible One-Way Hash | RISKY_CRYPTO |
| | 359 | Exposure of Private Personal Information to an Unauthorized Actor | SENSITIVE_DATA_LEAK, UNSAFE_BASIC_AUTH |
| A4: XML External Entity | 611 | Improper Restriction of XML External Entity Reference | XML_EXTERNAL_ENTITY |
| | 776 | Improper Restriction of Recursive Entity References in DTDs ('XML Entity Expansion') | XML_EXTERNAL_ENTITY |
| A5: Broken Access Control | 22 | Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') | PATH_MANIPULATION |
| | 284 | Improper Access Control | BAD_CERT_VERIFICATION, HARDCODED_CREDENTIALS, RISKY_CRYPTO, SENSITIVE_DATA_LEAK, SQLI, UNSAFE_BASIC_AUTH |
| | 285 | Improper Authorization | SQLI |
| | 639 | Authorization Bypass Through User-Controlled Key | SQLI |
| | 1031 | Broken Access Control | URL_MANIPULATION |
| A6: Security Misconfiguration | 16 | Configuration | SENSITIVE_DATA_LEAK |
| | 209 | Generation of Error Message Containing Sensitive Information | SENSITIVE_DATA_LEAK |
| A7: Cross-Site Scripting (XSS) | 79 | Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') | XSS |
| A8: Insecure Deserialization | 502 | Deserialization of Untrusted Data | DISTRUSTED_DATA_DESERIALIZATION |
| A10: Insufficient Logging & Monitoring | 223 | Omission of Security-relevant Information | INSUFFICIENT_LOGGING |
| | 778 | Insufficient Logging | INSUFFICIENT_LOGGING |

## Java

| Coverity Version 2021.03 -Java | | | |
|---|---|---|---|
| **Category** | **CWE** | **Description** | **Coverity Checker** |
| A1: Injection | 77 | Improper Neutralization of Special Elements used in a Command ('Command Injection') | CERT IDS07-J, EL_INJECTION, HEADER_INJECTION, MISSING_HEADER_VALIDATION, OS_CMD_INJECTION, TAINTED_ENVIRONMENT_WITH_EXECUTION |
| | 78 | Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection') | CERT IDS07-J, OS_CMD_INJECTION, TAINTED_ENVIRONMENT_WITH_EXECUTION |
| | 88 | Improper Neutralization of Argument Delimiters in a Command ('Argument Injection') | HEADER_INJECTION, MISSING_HEADER_VALIDATION, OS_CMD_INJECTION |
| | 89 | Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') | CONFIG.MYBATIS_MAPPER_SQLI, JSP_SQL_INJECTION, SQLI, SQL_NOT_CONSTANT |
| | 90 | Improper Neutralization of Special Elements used in an LDAP Query ('LDAP Injection') | LDAP_INJECTION, LDAP_NOT_CONSTANT |
| | 91 | XML Injection (aka Blind XPath Injection) | WEAK_XML_SCHEMA, XML_INJECTION, XPATH_INJECTION |
| | 564 | SQL Injection: Hibernate | CONFIG.MYBATIS_MAPPER_SQLI, JSP_SQL_INJECTION, SQLI, SQL_NOT_CONSTANT |
| | 917 | Improper Neutralization of Special Elements used in an Expression Language Statement ('Expression Language Injection') | EL_INJECTION |
| | 943 | Improper Neutralization of Special Elements in Data Query Logic | CONFIG.MYBATIS_MAPPER_SQLI, JSP_SQL_INJECTION, LDAP_INJECTION, LDAP_NOT_CONSTANT, SQLI, SQL_NOT_CONSTANT, XPATH_INJECTION |
| | 1027 | Injection | JAVA_CODE_INJECTION, JCR_INJECTION, JSP_DYNAMIC_INCLUDE, NOSQL_QUERY_INJECTION, OGNL_INJECTION, REGEX_INJECTION, SCRIPT_CODE_INJECTION, UNKNOWN_LANGUAGE_INJECTION, UNSAFE_JNI, UNSAFE_REFLECTION, URL_MANIPULATION |

| | | | |
|---|---|---|---|
| A2: Broken Authentication | 287 | Improper Authentication | CERT MSC03-J, CERT SEC02-J, CONFIG.HARDCODED_CREDENTIALS_AUDIT, CONFIG.MISSING_JSF2_SECURITY_CONSTRAINT, CONFIG.SPRING_BOOT_ADMIN_ACCESS_ENABLED, CONFIG.SPRING_BOOT_SSL_DISABLED, CONFIG.SPRING_SECURITY_HARDCODED_CREDENTIALS, CONFIG.SPRING_SECURITY_REMEMBER_ME_HARDCODED_KEY, CONFIG.SPRING_SECURITY_SESSION_FIXATION, CONFIG.SPRING_SECURITY_WEAK_PASSWORD_HASH, CONFIG.WEAK_SECURITY_CONSTRAINT, CORS_MISCONFIGURATION, CORS_MISCONFIGURATION_AUDIT, HARDCODED_CREDENTIALS, INSECURE_COMMUNICATION, MISSING_AUTHZ, SENSITIVE_DATA_LEAK, SESSION_FIXATION, UNENCRYPTED_SENSITIVE_DATA, WEAK_GUARD, WEAK_URL_SANITIZATION |
| | 256 | Unprotected Storage of Credentials | SENSITIVE_DATA_LEAK, UNENCRYPTED_SENSITIVE_DATA |
| | 384 | Session Fixation | CONFIG.SPRING_SECURITY_SESSION_FIXATION, SESSION_FIXATION |
| | 522 | Insufficiently Protected Credentials | CONFIG.HARDCODED_CREDENTIALS_AUDIT, INSECURE_COMMUNICATION, SENSITIVE_DATA_LEAK, UNENCRYPTED_SENSITIVE_DATA |
| | 523 | Unprotected Transport of Credentials | INSECURE_COMMUNICATION, SENSITIVE_DATA_LEAK, UNENCRYPTED_SENSITIVE_DATA |
| | 613 | Insufficient Session Expiration | CONFIG.UNSAFE_SESSION_TIMEOUT |
| | 1028 | Broken Authentication | CONFIG.SPRING_SECURITY_EXPOSED_SESSIONID, CONFIG.SPRING_SECURITY_LOGIN_OVER_HTTP, CONFIG.SPRING_SECURITY_UNSAFE_AUTHENTICATION_FILTER, DISABLED_ENCRYPTION, INSECURE_COOKIE, INSECURE_REMEMBER_ME_COOKIE, JSP_DYNAMIC_INCLUDE, VERBOSE_ERROR_REPORTING, WEAK_PASSWORD_HASH |

| | | | |
|---|---|---|---|
| A3: Sensitive Data Exposure | 295 | Improper Certificate Validation | BAD_CERT_VERIFICATION, CONFIG.SPRING_BOOT_SSL_DISABLED |
| | 311 | Missing Encryption of Sensitive Data | CONFIG.SPRING_BOOT_SSL_DISABLED, CONFIG.SPRING_SECURITY_LOGIN_OVER_HTTP, DISABLED_ENCRYPTION, HARDCODED_CREDENTIALS, INSECURE_COMMUNICATION, INSECURE_COOKIE, INSECURE_REMEMBER_ME_COOKIE, SENSITIVE_DATA_LEAK, UNENCRYPTED_SENSITIVE_DATA |
| | 312 | Cleartext Storage of Sensitive Information | HARDCODED_CREDENTIALS, SENSITIVE_DATA_LEAK, UNENCRYPTED_SENSITIVE_DATA |
| | 319 | Cleartext Transmission of Sensitive Information | CONFIG.SPRING_SECURITY_LOGIN_OVER_HTTP, DISABLED_ENCRYPTION, INSECURE_COMMUNICATION, SENSITIVE_DATA_LEAK, UNENCRYPTED_SENSITIVE_DATA |
| | 320 | Key Management Errors | HARDCODED_CREDENTIALS |
| | 326 | Inadequate Encryption Strength | CONFIG.SPRING_SECURITY_WEAK_PASSWORD_HASH, RISKY_CRYPTO |
| | 327 | Use of a Broken or Risky Cryptographic Algorithm | CONFIG.SPRING_SECURITY_WEAK_PASSWORD_HASH, RISKY_CRYPTO, WEAK_PASSWORD_HASH |
| | 328 | Reversible One-Way Hash | RISKY_CRYPTO |
| | 359 | Exposure of Private Personal Information to an Unauthorized Actor | CONFIG.SPRING_BOOT_SSL_DISABLED, CONFIG.SPRING_SECURITY_EXPOSED_SESSIONID, CONFIG.SPRING_SECURITY_LOGIN_OVER_HTTP, CONFIG.SPRING_SECURITY_UNSAFE_AUTHENTICATION_FILTER, CORS_MISCONFIGURATION_AUDIT, DISABLED_ENCRYPTION, INSECURE_COMMUNICATION, SENSITIVE_DATA_LEAK, UNENCRYPTED_SENSITIVE_DATA, VERBOSE_ERROR_REPORTING |
| | 1029 | Sensitive Data Exposure | CONFIG.DWR_DEBUG_MODE, CONFIG.DYNAMIC_DATA_HTML_COMMENT, CONFIG.JAVAEE_MISSING_HTTPONLY, CONFIG.SPRING_SECURITY_DEBUG_MODE |
| A4: XML External Entity | 611 | Improper Restriction of XML External Entity Reference | XML_EXTERNAL_ENTITY |
| | 776 | Improper Restriction of Recursive Entity References in DTDs ('XML Entity Expansion') | XML_EXTERNAL_ENTITY |

| | | | |
|---|---|---|---|
| A5: Broken Access Control<br><br>(cont. on next page) | 22 | Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') | JSP_DYNAMIC_INCLUDE, PATH_MANIPULATION |
| | 284 | Improper Access Control | ANDROID_CAPABILITY_LEAK, ANDROID_WEBVIEW_FILEACCESS, BAD_CERT_VERIFICATION, CERT ENV03-J, CERT MSC03-J, CERT SEC01-J, CERT SEC02-J, CERT SEC06-J, CERT SER08-J, CONFIG.DWR_DEBUG_MODE, CONFIG.HARDCODED_CREDENTIALS_AUDIT, CONFIG.JAVAEE_MISSING_SERVLET_MAPPING, CONFIG.MISSING_JSF2_SECURITY_CONSTRAINT, CONFIG.MYBATIS_MAPPER_SQLI, CONFIG.SPRING_BOOT_ADMIN_ACCESS_ENABLED, CONFIG.SPRING_BOOT_SSL_DISABLED, CONFIG.SPRING_SECURITY_DISABLE_AUTH_TAGS, CONFIG.SPRING_SECURITY_HARDCODED_CREDENTIALS, CONFIG.SPRING_SECURITY_REMEMBER_ME_HARDCODED_KEY, CONFIG.SPRING_SECURITY_SESSION_FIXATION, CONFIG.SPRING_SECURITY_WEAK_PASSWORD_HASH, CONFIG.STRUTS2_CONFIG_BROWSER_PLUGIN, CONFIG.STRUTS2_DYNAMIC_METHOD_INVOCATION, CONFIG.STRUTS2_ENABLED_DEV_MODE, CONFIG.UNSAFE_SESSION_TIMEOUT, CONFIG.WEAK_SECURITY_CONSTRAINT, CORS_MISCONFIGURATION, CORS_MISCONFIGURATION_AUDIT, HARDCODED_CREDENTIALS, IMPLICIT_INTENT, INSECURE_COMMUNICATION, INSECURE_REMEMBER_ME_COOKIE, JSP_SQL_INJECTION, MISSING_AUTHZ, MISSING_PERMISSION_FOR_BROADCAST, MISSING_PERMISSION_ON_EXPORTED_COMPONENT, RISKY_CRYPTO, SENSITIVE_DATA_LEAK, SESSION_FIXATION, SQLI, SQL_NOT_CONSTANT, UNENCRYPTED_SENSITIVE_DATA, WEAK_GUARD, WEAK_URL_SANITIZATION |

| | | | |
|---|---|---|---|
| A5: Broken Access Control<br>(cont.) | 285 | Improper Authorization | ANDROID_CAPABILITY_LEAK, CERT ENV03-J, CONFIG. DWR_DEBUG_MODE, CONFIG. JAVAEE_MISSING_SERVLET_ MAPPING, CONFIG.MISSING_ JSF2_SECURITY_CONSTRAINT, CONFIG.MYBATIS_MAPPER_SQLI, CONFIG.SPRING_BOOT_SSL_ DISABLED, CONFIG.SPRING_ SECURITY_DISABLE_AUTH_TAGS, CONFIG.STRUTS2_CONFIG_ BROWSER_PLUGIN, CONFIG. STRUTS2_DYNAMIC_METHOD_ INVOCATION, CONFIG.STRUTS2_ ENABLED_DEV_MODE, CONFIG. WEAK_SECURITY_CONSTRAINT, CORS_MISCONFIGURATION, CORS_MISCONFIGURATION_ AUDIT, IMPLICIT_INTENT, JSP_SQL_INJECTION, MISSING_AUTHZ, MISSING_ PERMISSION_FOR_BROADCAST, MISSING_PERMISSION_ON_ EXPORTED_COMPONENT, SENSITIVE_DATA_LEAK, SQLI, SQL_NOT_CONSTANT |
| | 425 | Direct Request (‘Forced Browsing’) | CONFIG.MISSING_JSF2_ SECURITY_CONSTRAINT |
| | 639 | Authorization Bypass Through User-Controlled Key | CONFIG.MYBATIS_MAPPER_SQLI, JSP_SQL_INJECTION, SQLI, SQL_ NOT_CONSTANT |
| | 1031 | Broken Access Control | URL_MANIPULATION |

| | | | |
|---|---|---|---|
| A6: Security Misconfiguration | 16 | Configuration | CONFIG.DUPLICATE_SERVLET_DEFINITION, CONFIG.DWR_DEBUG_MODE, CONFIG.HTTP_VERB_TAMPERING, CONFIG.JAVAEE_MISSING_HTTPONLY, CONFIG.MISSING_GLOBAL_EXCEPTION_HANDLER, CONFIG.MISSING_JSF2_SECURITY_CONSTRAINT, CONFIG.SPRING_SECURITY_DEBUG_MODE, CONFIG.SPRING_SECURITY_DISABLE_AUTH_TAGS, CONFIG.SPRING_SECURITY_HARDCODED_CREDENTIALS, CONFIG.SPRING_SECURITY_LOGIN_OVER_HTTP, CONFIG.SPRING_SECURITY_REMEMBER_ME_HARDCODED_KEY, CONFIG.SPRING_SECURITY_SESSION_FIXATION, CONFIG.STRUTS2_CONFIG_BROWSER_PLUGIN, CONFIG.STRUTS2_DYNAMIC_METHOD_INVOCATION, CONFIG.STRUTS2_ENABLED_DEV_MODE, CONFIG.UNSAFE_SESSION_TIMEOUT, INSECURE_COMMUNICATION, INSECURE_HTTP_FIREWALL, SENSITIVE_DATA_LEAK, UNENCRYPTED_SENSITIVE_DATA |
| | 209 | Generation of Error Message Containing Sensitive Information | SENSITIVE_DATA_LEAK, VERBOSE_ERROR_REPORTING |
| | 1032 | Security Misconfiguration | CONFIG.ANDROID_OUTDATED_TARGETSDKVERSION |
| A7: Cross-Site Scripting (XSS) | 79 | Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') | CONFIG.SPRING_SECURITY_DEPRECATED_XSS_HEADER, XSS |
| A8: Insecure Deserialization | 502 | Deserialization of Untrusted Data | CERT SER01-J, UNSAFE_DESERIALIZATION |
| A9: Using Components with Known Vulnerabilities | 1035 | Using Components With Known Vulnerabilities | CONFIG.ANDROID_UNSAFE_MINSDKVERSION |
| A10: Insufficient Logging & Monitoring | 223 | Omission of Security-relevant Information | UNLOGGED_SECURITY_EXCEPTION |
| | 778 | Insufficient Logging | UNLOGGED_SECURITY_EXCEPTION |

## JavaScript

| Coverity Version 2021.03 - JavaScript | | | |
|---|---|---|---|
| **Category** | **CWE** | **Description** | **Coverity Checker** |
| A1: Injection | 77 | Improper Neutralization of Special Elements used in a Command ('Command Injection') | HEADER_INJECTION, OS_CMD_INJECTION, TAINTED_ENVIRONMENT_WITH_EXECUTION |
| | 78 | Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection') | OS_CMD_INJECTION, TAINTED_ENVIRONMENT_WITH_EXECUTION |
| | 88 | Improper Neutralization of Argument Delimiters in a Command ('Argument Injection') | HEADER_INJECTION, OS_CMD_INJECTION |
| | 89 | Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') | SQLI |
| | 943 | Improper Neutralization of Special Elements in Data Query Logic | SQLI |
| | 1027 | Injection | ANGULAR_EXPRESSION_INJECTION, NOSQL_QUERY_INJECTION, REGEX_INJECTION, SCRIPT_CODE_INJECTION, URL_MANIPULATION |
| A2: Broken Authentication<br>(cont. on next page) | 287 | Improper Authentication | AWS_SSL_DISABLED, AWS_VALIDATION_DISABLED, CONFIG.COOKIE_SIGNING_DISABLED, CONFIG.HARDCODED_CREDENTIALS_AUDIT, CONFIG.HARDCODED_TOKEN, CONFIG.SEQUELIZE_INSECURE_CONNECTION, CORS_MISCONFIGURATION, CORS_MISCONFIGURATION_AUDIT, HARDCODED_CREDENTIALS, HPKP_MISCONFIGURATION, INSECURE_COMMUNICATION, MISSING_AUTHZ, MULTER_MISCONFIGURATION, SENSITIVE_DATA_LEAK, UNLESS_CASE_SENSITIVE_ROUTE_MATCHING, WEAK_URL_SANITIZATION |
| | 256 | Unprotected Storage of Credentials | SENSITIVE_DATA_LEAK |
| | 522 | Insufficiently Protected Credentials | AWS_SSL_DISABLED, CONFIG.HARDCODED_CREDENTIALS_AUDIT, CONFIG.HARDCODED_TOKEN, CONFIG.SEQUELIZE_INSECURE_CONNECTION, INSECURE_COMMUNICATION, SENSITIVE_DATA_LEAK |
| | 523 | Unprotected Transport of Credentials | AWS_SSL_DISABLED, CONFIG.SEQUELIZE_INSECURE_CONNECTION, INSECURE_COMMUNICATION, SENSITIVE_DATA_LEAK |

| | | | |
|---|---|---|---|
| A2: Broken Authentication (cont.) | 613 | Insufficient Session Expiration | CONFIG.JSONWEBTOKEN_NON_EXPIRING_TOKEN, CONFIG.UNSAFE_SESSION_TIMEOUT, CORS_MISCONFIGURATION_AUDIT, HPKP_MISCONFIGURATION, INSUFFICIENT_PRESIGNED_URL_TIMEOUT, JSONWEBTOKEN_IGNORED_EXPIRATION_TIME, TEMPORARY_CREDENTIALS_DURATION |
| | 1028 | Broken Authentication | INSECURE_ACL, INSECURE_COOKIE, INSECURE_REFERRER_POLICY, REVERSE_TABNABBING, UNSAFE_BUFFER_METHOD |
| A3: Sensitive Data Exposure | 295 | Improper Certificate Validation | AWS_VALIDATION_DISABLED, BAD_CERT_VERIFICATION, CONFIG.MYSQL_SSL_VERIFY_DISABLED, CONFIG.REQUEST_STRICTSSL_DISABLED, HPKP_MISCONFIGURATION |
| | 311 | Missing Encryption of Sensitive Data | AWS_SSL_DISABLED, CONFIG.SEQUELIZE_INSECURE_CONNECTION, HAPI_SESSION_MONGO_MISSING_TLS, INSECURE_COMMUNICATION, INSECURE_COOKIE, SENSITIVE_DATA_LEAK |
| | 312 | Cleartext Storage of Sensitive Information | SENSITIVE_DATA_LEAK |
| | 319 | Cleartext Transmission of Sensitive Information | AWS_SSL_DISABLED, CONFIG.SEQUELIZE_INSECURE_CONNECTION, HAPI_SESSION_MONGO_MISSING_TLS, INSECURE_COMMUNICATION, SENSITIVE_DATA_LEAK |
| | 326 | Inadequate Encryption Strength | RISKY_CRYPTO |
| | 327 | Use of a Broken or Risky Cryptographic Algorithm | INSECURE_SALT, RISKY_CRYPTO, SA.RISKY_CRYPTO |
| | 328 | Reversible One-Way Hash | RISKY_CRYPTO |
| | 359 | Exposure of Private Personal Information to an Unauthorized Actor | AWS_SSL_DISABLED, CORS_MISCONFIGURATION, CORS_MISCONFIGURATION_AUDIT, HPKP_MISCONFIGURATION, INSECURE_ACL, INSECURE_COMMUNICATION, INSECURE_REFERRER_POLICY, REVERSE_TABNABBING, SENSITIVE_DATA_LEAK, UNSAFE_BUFFER_METHOD |
| | 1029 | Sensitive Data Exposure | CONFIG.ENABLED_DEBUG_MODE, CONFIG.SEQUELIZE_ENABLED_LOGGING, CONFIG.VUE_ROUTER_PARAMS_EXPOSED_TO_PROPS, EXPOSED_DIRECTORY_LISTING, EXPRESS_X_POWERED_BY_ENABLED, INSECURE_COOKIE |

| | | | |
|---|---|---|---|
| A4: XML External Entity | 611 | Improper Restriction of XML External Entity Reference | XML_EXTERNAL_ENTITY |
| | 776 | Improper Restriction of Recursive Entity References in DTDs ('XML Entity Expansion') | XML_EXTERNAL_ENTITY |
| A5: Broken Access Control | 22 | Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') | BUSBOY_MISCONFIGURATION, FILE_UPLOAD_ MISCONFIGURATION, MULTER_ MISCONFIGURATION, PATH_ MANIPULATION |
| | 284 | Improper Access Control | AWS_SSL_DISABLED, AWS_ VALIDATION_DISABLED, BAD_ CERT_VERIFICATION, CONFIG. COOKIE_SIGNING_DISABLED, CONFIG.HARDCODED_ CREDENTIALS_AUDIT, CONFIG. HARDCODED_TOKEN, CONFIG. REQUEST_STRICTSSL_DISABLED, CONFIG.SEQUELIZE_INSECURE_ CONNECTION, CONFIG. UNSAFE_SESSION_TIMEOUT, CORS_MISCONFIGURATION, CORS_MISCONFIGURATION_ AUDIT, HARDCODED_ CREDENTIALS, HPKP_ MISCONFIGURATION, INSECURE_ACL, INSECURE_ COMMUNICATION, INSECURE_ COOKIE, INSUFFICIENT_ PRESIGNED_URL_TIMEOUT, MISSING_AUTHZ, MULTER_ MISCONFIGURATION, RISKY_ CRYPTO, SA.RISKY_CRYPTO, SENSITIVE_DATA_LEAK, SQLI, TEMPORARY_CREDENTIALS_ DURATION, UNCHECKED_ORIGIN, UNLESS_CASE_SENSITIVE_ ROUTE_MATCHING, WEAK_URL_ SANITIZATION |
| | 285 | Improper Authorization | AWS_VALIDATION_DISABLED, CONFIG.COOKIE_SIGNING_ DISABLED, CORS_ MISCONFIGURATION, CORS_ MISCONFIGURATION_AUDIT, HPKP_MISCONFIGURATION, INSECURE_ACL, INSECURE_ COOKIE, MISSING_AUTHZ, SQLI |
| | 639 | Authorization Bypass Through User-Controlled Key | SQLI |
| | 1031 | Broken Access Control | URL_MANIPULATION |

| | | | |
|---|---|---|---|
| A6: Security Misconfiguration | 16 | Configuration | CONFIG.ENABLED_DEBUG_MODE, CONFIG.HANA_XS_PREVENT_XSRF_DISABLED, CONFIG.MISSING_GLOBAL_EXCEPTION_HANDLER, CONFIG.UNSAFE_SESSION_TIMEOUT, CORS_MISCONFIGURATION_AUDIT, HPKP_MISCONFIGURATION, INSUFFICIENT_PRESIGNED_URL_TIMEOUT, SENSITIVE_DATA_LEAK, TEMPORARY_CREDENTIALS_DURATION |
| | 209 | Generation of Error Message Containing Sensitive Information | SENSITIVE_DATA_LEAK |
| | 548 | Exposure of Information Through Directory Listing | EXPOSED_DIRECTORY_LISTING |
| A7: Cross-Site Scripting (XSS) | 79 | Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') | ANGULAR_BYPASS_SECURITY, ANGULAR_ELEMENT_REFERENCE, ANGULAR_SCE_DISABLED, DOM_XSS, REACT_DANGEROUS_INNERHTML, VUE_TEMPLATE_UNSAFE_VHTML_DIRECTIVE, XSS |
| A8: Insecure Deserialization | 502 | Deserialization of Untrusted Data | UNSAFE_DESERIALIZATION |
| A10: Insufficient Logging & Monitoring | 223 | Omission of Security-relevant Information | INSUFFICIENT_LOGGING |
| | 778 | Insufficient Logging | INSUFFICIENT_LOGGING |

## Kotlin

| Coverity Version 2021.03 - Kotlin | | | |
|---|---|---|---|
| **Category** | **CWE** | **Description** | **Coverity Checker** |
| A1: Injection | 77 | Improper Neutralization of Special Elements used in a Command ('Command Injection') | HEADER_INJECTION, OS_CMD_INJECTION |
| | 78 | Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection') | OS_CMD_INJECTION |
| | 88 | Improper Neutralization of Argument Delimiters in a Command ('Argument Injection') | HEADER_INJECTION, OS_CMD_INJECTION |
| | 89 | Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') | SQLI |
| | 91 | XML Injection (aka Blind XPath Injection) | XPATH_INJECTION |
| | 943 | Improper Neutralization of Special Elements in Data Query Logic | SQLI, XPATH_INJECTION |
| | 1027 | Injection | REGEX_INJECTION, UNSAFE_JNI, URL_MANIPULATION |
| A2: Broken Authentication<br>(cont. on next page) | 287 | Improper Authentication | HARDCODED_CREDENTIALS, INSECURE_COMMUNICATION, SENSITIVE_DATA_LEAK, UNENCRYPTED_SENSITIVE_DATA |
| | 256 | Unprotected Storage of Credentials | SENSITIVE_DATA_LEAK, UNENCRYPTED_SENSITIVE_DATA |
| | 522 | Insufficiently Protected Credentials | INSECURE_COMMUNICATION, SENSITIVE_DATA_LEAK, UNENCRYPTED_SENSITIVE_DATA |

| | | | |
|---|---|---|---|
| A2: Broken Authentication (cont.) | 523 | Unprotected Transport of Credentials | INSECURE_COMMUNICATION, SENSITIVE_DATA_LEAK, UNENCRYPTED_SENSITIVE_DATA |
| | 1028 | Broken Authentication | WEAK_PASSWORD_HASH |
| A3: Sensitive Data Exposure | 295 | Improper Certificate Validation | BAD_CERT_VERIFICATION |
| | 311 | Missing Encryption of Sensitive Data | HARDCODED_CREDENTIALS, INSECURE_COMMUNICATION, SENSITIVE_DATA_LEAK, UNENCRYPTED_SENSITIVE_DATA |
| | 312 | Cleartext Storage of Sensitive Information | HARDCODED_CREDENTIALS, SENSITIVE_DATA_LEAK, UNENCRYPTED_SENSITIVE_DATA |
| | 319 | Cleartext Transmission of Sensitive Information | INSECURE_COMMUNICATION, SENSITIVE_DATA_LEAK, UNENCRYPTED_SENSITIVE_DATA |
| | 320 | Key Management Errors | HARDCODED_CREDENTIALS |
| | 326 | Inadequate Encryption Strength | RISKY_CRYPTO |
| | 327 | Use of a Broken or Risky Cryptographic Algorithm | RISKY_CRYPTO, WEAK_ PASSWORD_HASH |
| | 328 | Reversible One-Way Hash | RISKY_CRYPTO |
| | 359 | Exposure of Private Personal Information to an Unauthorized Actor | SENSITIVE_DATA_LEAK, UNENCRYPTED_SENSITIVE_DATA |
| A4: XML External Entity | 611 | Improper Restriction of XML External Entity Reference | XML_EXTERNAL_ENTITY |
| | 776 | Improper Restriction of Recursive Entity References in DTDs ('XML Entity Expansion') | XML_EXTERNAL_ENTITY |
| A5: Broken Access Control | 22 | Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') | PATH_MANIPULATION |
| | 284 | Improper Access Control | ANDROID_CAPABILITY_LEAK, BAD_CERT_VERIFICATION, HARDCODED_CREDENTIALS, IMPLICIT_INTENT, INSECURE_COMMUNICATION, MISSING_PERMISSION_FOR_ BROADCAST, RISKY_CRYPTO, SENSITIVE_DATA_LEAK, SQLI, UNENCRYPTED_SENSITIVE_DATA |
| | 285 | Improper Authorization | ANDROID_CAPABILITY_LEAK, IMPLICIT_INTENT, MISSING_ PERMISSION_FOR_BROADCAST, SENSITIVE_DATA_LEAK, SQLI |
| | 639 | Authorization Bypass Through User-Controlled Key | SQLI |
| | 1031 | Broken Access Control | URL_MANIPULATION |
| A6: Security Misconfiguration | 16 | Configuration | INSECURE_COMMUNICATION, SENSITIVE_DATA_LEAK, UNENCRYPTED_SENSITIVE_DATA |
| | 209 | Generation of Error Message Containing Sensitive Information | SENSITIVE_DATA_LEAK |
| | 1032 | Security Misconfiguration | CONFIG.ANDROID_OUTDATED_ TARGETSDKVERSION |
| A8: Insecure Deserialization | 502 | Deserialization of Untrusted Data | UNSAFE_DESERIALIZATION |

| | | | |
|---|---|---|---|
| A9: Using Components with Known Vulnerabilities | 1035 | Using Components With Known Vulnerabilities | CONFIG.ANDROID_UNSAFE_MINSDKVERSION |
| A10: Insufficient Logging & Monitoring | 223 | Omission of Security-relevant Information | UNLOGGED_SECURITY_EXCEPTION |
| | 778 | Insufficient Logging | UNLOGGED_SECURITY_EXCEPTION |

## PHP

| Coverity Version 2021.03 - PHP | | | |
|---|---|---|---|
| **Category** | **CWE** | **Description** | **Coverity Checker** |
| A1: Injection | 77 | Improper Neutralization of Special Elements used in a Command ('Command Injection') | HEADER_INJECTION, OS_CMD_INJECTION |
| | 78 | Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection') | OS_CMD_INJECTION |
| | 88 | Improper Neutralization of Argument Delimiters in a Command ('Argument Injection') | HEADER_INJECTION, OS_CMD_INJECTION |
| | 89 | Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') | SQLI |
| | 943 | Improper Neutralization of Special Elements in Data Query Logic | SQLI |
| | 1027 | Injection | NOSQL_QUERY_INJECTION, SCRIPT_CODE_INJECTION, SYMFONY_EL_INJECTION, UNSAFE_REFLECTION |
| A2: Broken Authentication | 287 | Improper Authentication | HARDCODED_CREDENTIALS, MISSING_AUTHZ, SENSITIVE_DATA_LEAK |
| | 256 | Unprotected Storage of Credentials | SENSITIVE_DATA_LEAK |
| | 522 | Insufficiently Protected Credentials | SENSITIVE_DATA_LEAK |
| | 523 | Unprotected Transport of Credentials | SENSITIVE_DATA_LEAK |
| A3: Sensitive Data Exposure | 311 | Missing Encryption of Sensitive Data | SENSITIVE_DATA_LEAK |
| | 312 | Cleartext Storage of Sensitive Information | SENSITIVE_DATA_LEAK |
| | 319 | Cleartext Transmission of Sensitive Information | SENSITIVE_DATA_LEAK |
| | 359 | Exposure of Private Personal Information to an Unauthorized Actor | SENSITIVE_DATA_LEAK |
| A4: XML External Entity | 611 | Improper Restriction of XML External Entity Reference | XML_EXTERNAL_ENTITY |
| A5: Broken Access Control | 22 | Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') | PATH_MANIPULATION |
| | 284 | Improper Access Control | HARDCODED_CREDENTIALS, MISSING_AUTHZ, SENSITIVE_DATA_LEAK, SQLI |
| | 285 | Improper Authorization | MISSING_AUTHZ, SQLI |
| | 639 | Authorization Bypass Through User-Controlled Key | SQLI |

| | | | |
|---|---|---|---|
| A6: Security Misconfiguration | 16 | Configuration | CONFIG.SYMFONY_CSRF_PROTECTION_DISABLED, SENSITIVE_DATA_LEAK |
| | 209 | Generation of Error Message Containing Sensitive Information | SENSITIVE_DATA_LEAK |
| A7: Cross-Site Scripting (XSS) | 79 | Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') | XSS |
| A8: Insecure Deserialization | 502 | Deserialization of Untrusted Data | UNSAFE_DESERIALIZATION |

## Python

| Coverity Version 2021.03 - Python | | | |
|---|---|---|---|
| **Category** | **CWE** | **Description** | **Coverity Checker** |
| A1: Injection | 77 | Improper Neutralization of Special Elements used in a Command ('Command Injection') | HEADER_INJECTION, OS_CMD_INJECTION |
| | 78 | Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection') | OS_CMD_INJECTION |
| | 88 | Improper Neutralization of Argument Delimiters in a Command ('Argument Injection') | HEADER_INJECTION, OS_CMD_INJECTION |
| | 89 | Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') | SQLI |
| | 943 | Improper Neutralization of Special Elements in Data Query Logic | SQLI |
| | 1027 | Injection | NOSQL_QUERY_INJECTION, REGEX_INJECTION, SCRIPT_CODE_INJECTION, URL_MANIPULATION |
| A2: Broken Authentication | 287 | Improper Authentication | ANONYMOUS_DB_CONNECTION, HARDCODED_CREDENTIALS, HOST_HEADER_VALIDATION_DISABLED, MISSING_AUTHZ, MISSING_PASSWORD_VALIDATOR, SENSITIVE_DATA_LEAK, WEAK_URL_SANITIZATION |
| | 256 | Unprotected Storage of Credentials | SENSITIVE_DATA_LEAK |
| | 522 | Insufficiently Protected Credentials | SENSITIVE_DATA_LEAK |
| | 523 | Unprotected Transport of Credentials | SENSITIVE_DATA_LEAK |
| | 1028 | Broken Authentication | INSECURE_COMMUNICATION, INSECURE_COOKIE, INSECURE_NETWORK_BIND, INSECURE_REFERRER_POLICY, SECURE_TEMP, WEAK_PASSWORD_HASH |
| A3: Sensitive Data Exposure<br>(cont. on next page) | 295 | Improper Certificate Validation | BAD_CERT_VERIFICATION |
| | 311 | Missing Encryption of Sensitive Data | INSECURE_COMMUNICATION, INSECURE_COOKIE, SENSITIVE_DATA_LEAK |
| | 312 | Cleartext Storage of Sensitive Information | SENSITIVE_DATA_LEAK |
| | 319 | Cleartext Transmission of Sensitive Information | INSECURE_COMMUNICATION, SENSITIVE_DATA_LEAK |
| | 326 | Inadequate Encryption Strength | RISKY_CRYPTO |

| | | | |
|---|---|---|---|
| A3: Sensitive Data Exposure (cont.) | 327 | Use of a Broken or Risky Cryptographic Algorithm | INSECURE_SALT, RISKY_CRYPTO, WEAK_PASSWORD_HASH |
| | 328 | Reversible One-Way Hash | RISKY_CRYPTO |
| | 359 | Exposure of Private Personal Information to an Unauthorized Actor | INSECURE_COMMUNICATION, INSECURE_NETWORK_BIND, INSECURE_REFERRER_POLICY, SECURE_TEMP, SENSITIVE_DATA_LEAK |
| | 1029 | Sensitive Data Exposure | CONFIG.ENABLED_DEBUG_MODE |
| A4: XML External Entity | 611 | Improper Restriction of XML External Entity Reference | XML_EXTERNAL_ENTITY |
| A5: Broken Access Control | 22 | Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') | PATH_MANIPULATION |
| | 284 | Improper Access Control | ANONYMOUS_DB_CONNECTION, BAD_CERT_VERIFICATION, HARDCODED_CREDENTIALS, HOST_HEADER_VALIDATION_DISABLED, INSECURE_COOKIE, MISSING_AUTHZ, MISSING_PASSWORD_VALIDATOR, RISKY_CRYPTO, SENSITIVE_DATA_LEAK, SQLI, WEAK_URL_SANITIZATION |
| | 285 | Improper Authorization | ANONYMOUS_DB_CONNECTION, INSECURE_COOKIE, MISSING_AUTHZ, SQLI |
| | 639 | Authorization Bypass Through User-Controlled Key | SQLI |
| | 1031 | Broken Access Control | URL_MANIPULATION |
| A6: Security Misconfiguration | 16 | Configuration | CONFIG.ENABLED_DEBUG_MODE, SENSITIVE_DATA_LEAK |
| | 209 | Generation of Error Message Containing Sensitive Information | SENSITIVE_DATA_LEAK |
| A7: Cross-Site Scripting (XSS) | 79 | Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') | JINJA2_AUTOESCAPE_DISABLED, XSS |
| A8: Insecure Deserialization | 502 | Deserialization of Untrusted Data | UNSAFE_DESERIALIZATION |
| A10: Insufficient Logging & Monitoring | 223 | Omission of Security-relevant Information | INSUFFICIENT_LOGGING |
| | 778 | Insufficient Logging | INSUFFICIENT_LOGGING |

## Ruby

| Coverity Version 2021.03 - Ruby | | | |
|---|---|---|---|
| **Category** | **CWE** | **Description** | **Coverity Checker** |
| A1: Injection (cont. on next page) | 77 | Improper Neutralization of Special Elements used in a Command ('Command Injection') | OS_CMD_INJECTION |
| | 78 | Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection') | OS_CMD_INJECTION |
| | 88 | Improper Neutralization of Argument Delimiters in a Command ('Argument Injection') | OS_CMD_INJECTION |
| | 89 | Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') | DYNAMIC_OBJECT_ATTRIBUTES, RUBY_VULNERABLE_LIBRARY, SQLI |

| | | | |
|---|---|---|---|
| A1: Injection (cont.) | 943 | Improper Neutralization of Special Elements in Data Query Logic | DYNAMIC_OBJECT_ATTRIBUTES, RUBY_VULNERABLE_LIBRARY, SQLI |
| | 1027 | Injection | REGEX_INJECTION, SCRIPT_CODE_INJECTION, UNSAFE_REFLECTION |
| A2: Broken Authentication | 287 | Improper Authentication | HARDCODED_CREDENTIALS, RAILS_DEVISE_CONFIG, RUBY_VULNERABLE_LIBRARY, STRICT_TRANSPORT_SECURITY, UNSAFE_BASIC_AUTH, UNSAFE_SESSION_SETTING |
| | 522 | Insufficiently Protected Credentials | STRICT_TRANSPORT_SECURITY |
| | 523 | Unprotected Transport of Credentials | STRICT_TRANSPORT_SECURITY |
| | 1028 | Broken Authentication | SENSITIVE_DATA_LEAK, WEAK_PASSWORD_HASH |
| A3: Sensitive Data Exposure | 295 | Improper Certificate Validation | BAD_CERT_VERIFICATION |
| | 311 | Missing Encryption of Sensitive Data | HARDCODED_CREDENTIALS, INSECURE_COOKIE, STRICT_TRANSPORT_SECURITY, UNSAFE_SESSION_SETTING |
| | 312 | Cleartext Storage of Sensitive Information | HARDCODED_CREDENTIALS |
| | 319 | Cleartext Transmission of Sensitive Information | STRICT_TRANSPORT_SECURITY |
| | 320 | Key Management Errors | UNSAFE_SESSION_SETTING |
| | 327 | Use of a Broken or Risky Cryptographic Algorithm | RAILS_DEVISE_CONFIG, WEAK_PASSWORD_HASH |
| | 359 | Exposure of Private Personal Information to an Unauthorized Actor | SENSITIVE_DATA_LEAK |
| A5: Broken Access Control | 22 | Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') | PATH_MANIPULATION, RUBY_VULNERABLE_LIBRARY |
| | 284 | Improper Access Control | BAD_CERT_VERIFICATION, HARDCODED_CREDENTIALS, INSECURE_COOKIE, INSECURE_DIRECT_OBJECT_REFERENCE, RAILS_DEFAULT_ROUTES, RAILS_DEVISE_CONFIG, RAILS_MISSING_FILTER_ACTION, RUBY_VULNERABLE_LIBRARY, STRICT_TRANSPORT_SECURITY, UNSAFE_BASIC_AUTH, UNSAFE_SESSION_SETTING |
| | 285 | Improper Authorization | INSECURE_COOKIE, INSECURE_DIRECT_OBJECT_REFERENCE, RAILS_DEFAULT_ROUTES, RAILS_MISSING_FILTER_ACTION, UNSAFE_SESSION_SETTING |
| | 639 | Authorization Bypass Through User-Controlled Key | INSECURE_DIRECT_OBJECT_REFERENCE |
| A6: Security Misconfiguration | 209 | Generation of Error Message Containing Sensitive Information | SENSITIVE_DATA_LEAK |
| A7: Cross-Site Scripting (XSS) | 79 | Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') | RUBY_VULNERABLE_LIBRARY, TEMPLATE_INJECTION, UNESCAPED_HTML, XSS |

| | | | |
|---|---|---|---|
| A8: Insecure Deserialization | 502 | Deserialization of Untrusted Data | COOKIE_SERIALIZER_CONFIG, RUBY_VULNERABLE_LIBRARY, UNSAFE_DESERIALIZATION |
| A9: Using Components with Known Vulnerabilities | 1035 | Using Components With Known Vulnerabilities | RUBY_VULNERABLE_LIBRARY |

## VB.NET

| Coverity Version 2021.03 - VB.NET | | | |
|---|---|---|---|
| **Category** | **CWE** | **Description** | **Coverity Checker** |
| A1: Injection | 77 | Improper Neutralization of Special Elements used in a Command ('Command Injection') | HEADER_INJECTION, OS_CMD_INJECTION |
| | 78 | Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection') | OS_CMD_INJECTION |
| | 88 | Improper Neutralization of Argument Delimiters in a Command ('Argument Injection') | HEADER_INJECTION, OS_CMD_INJECTION |
| | 89 | Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') | SQLI, SQL_NOT_CONSTANT |
| | 90 | Improper Neutralization of Special Elements used in an LDAP Query ('LDAP Injection') | LDAP_INJECTION, LDAP_NOT_CONSTANT |
| | 91 | XML Injection (aka Blind XPath Injection) | XML_INJECTION, XPATH_INJECTION |
| | 943 | Improper Neutralization of Special Elements in Data Query Logic | LDAP_INJECTION, LDAP_NOT_CONSTANT, SQLI, SQL_NOT_CONSTANT, XPATH_INJECTION |
| | 1027 | Injection | REGEX_INJECTION, SCRIPT_CODE_INJECTION |
| A2: Broken Authentication | 287 | Improper Authentication | HARDCODED_CREDENTIALS, INSECURE_COMMUNICATION, MISSING_AUTHZ, SENSITIVE_DATA_LEAK, UNENCRYPTED_SENSITIVE_DATA |
| | 256 | Unprotected Storage of Credentials | SENSITIVE_DATA_LEAK, UNENCRYPTED_SENSITIVE_DATA |
| | 522 | Insufficiently Protected Credentials | INSECURE_COMMUNICATION, SENSITIVE_DATA_LEAK, UNENCRYPTED_SENSITIVE_DATA |
| | 523 | Unprotected Transport of Credentials | INSECURE_COMMUNICATION, SENSITIVE_DATA_LEAK, UNENCRYPTED_SENSITIVE_DATA |
| | 1028 | Broken Authentication | WEAK_PASSWORD_HASH |
| A3: Sensitive Data Exposure<br>(cont. on next page) | 311 | Missing Encryption of Sensitive Data | HARDCODED_CREDENTIALS, INSECURE_COMMUNICATION, SENSITIVE_DATA_LEAK, UNENCRYPTED_SENSITIVE_DATA |
| | 312 | Cleartext Storage of Sensitive Information | HARDCODED_CREDENTIALS, SENSITIVE_DATA_LEAK, UNENCRYPTED_SENSITIVE_DATA |
| | 319 | Cleartext Transmission of Sensitive Information | INSECURE_COMMUNICATION, SENSITIVE_DATA_LEAK, UNENCRYPTED_SENSITIVE_DATA |

| | | | |
|---|---|---|---|
| A3: Sensitive Data Exposure (cont.) | 320 | Key Management Errors | HARDCODED_CREDENTIALS |
| | 326 | Inadequate Encryption Strength | RISKY_CRYPTO |
| | 327 | Use of a Broken or Risky Cryptographic Algorithm | RISKY_CRYPTO, WEAK_PASSWORD_HASH |
| | 328 | Reversible One-Way Hash | RISKY_CRYPTO |
| | 359 | Exposure of Private Personal Information to an Unauthorized Actor | SENSITIVE_DATA_LEAK, UNENCRYPTED_SENSITIVE_DATA |
| | 1029 | Sensitive Data Exposure | ASPNET_MVC_VERSION_HEADER, CONFIG.DYNAMIC_DATA_HTML_COMMENT |
| A4: XML External Entity | 611 | Improper Restriction of XML External Entity Reference | XML_EXTERNAL_ENTITY |
| | 776 | Improper Restriction of Recursive Entity References in DTDs ('XML Entity Expansion') | XML_EXTERNAL_ENTITY |
| A5: Broken Access Control | 22 | Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') | PATH_MANIPULATION |
| | 284 | Improper Access Control | HARDCODED_CREDENTIALS, INSECURE_COMMUNICATION, MISSING_AUTHZ, RISKY_CRYPTO, SENSITIVE_DATA_LEAK, SQLI, SQL_NOT_CONSTANT, UNENCRYPTED_SENSITIVE_DATA |
| | 285 | Improper Authorization | MISSING_AUTHZ, SQLI, SQL_NOT_CONSTANT |
| | 639 | Authorization Bypass Through User-Controlled Key | SQLI, SQL_NOT_CONSTANT |
| A6: Security Misconfiguration | 16 | Configuration | CONFIG.MISSING_CUSTOM_ERROR_PAGE, INSECURE_COMMUNICATION, SENSITIVE_DATA_LEAK, UNENCRYPTED_SENSITIVE_DATA |
| | 209 | Generation of Error Message Containing Sensitive Information | SENSITIVE_DATA_LEAK |
| A7: Cross-Site Scripting (XSS) | 79 | Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') | XSS |
| A8: Insecure Deserialization | 502 | Deserialization of Untrusted Data | UNSAFE_DESERIALIZATION |
| A10: Insufficient Logging & Monitoring | 223 | Omission of Security-relevant Information | UNLOGGED_SECURITY_EXCEPTION |
| | 778 | Insufficient Logging | UNLOGGED_SECURITY_EXCEPTION |

## The Synopsys difference

Synopsys helps development teams build secure, high-quality software, minimizing risks while maximizing speed and productivity. Synopsys, a recognized leader in application security, provides static analysis, software composition analysis, and dynamic analysis solutions that enable teams to quickly find and fix vulnerabilities and defects in proprietary code, open source components, and application behavior.

For more information about the Synopsys Software Integrity Group, visit us online at www.synopsys.com/software.

**Synopsys, Inc.**
185 Berry Street, Suite 6500
San Francisco, CA 94107 USA

U.S. Sales: 800.873.8193
International Sales: +1 415.321.5237
Email: sig-info@synopsys.com